Improving Cybersecurity for Smart Home Systems

Tauheed Waheed[a], Eda Marchetti[b] and Antonello Calabrò[c]
CNR-ISTI Pisa, Italy

Keywords: Cybersecurity, Smart Home Systems, Testing, User-Centric.

Abstract: Smart home systems consist of various interconnected devices that can be vulnerable to security risks, potentially compromising the integrity of the entire system. This paper aims to address cybersecurity challenges and identify research gaps to enhance cybersecurity for smart home systems. We aim to highlight the significance and impact of testing on smart home systems, with a focus on the drawbacks of current testing strategies. The limitations in current testing methodologies have identified the lack of user involvement in the testing process. We have proposed our user-centric SCTM (Smart-home Cybersecurity Testing Methodology) and its behavioral model to leverage cybersecurity in smart home systems.

1 INTRODUCTION

IoT is revolutionizing our everyday lives by allowing the easy use of a wide range of smart devices to improve our lifestyle, convenience, efficiency, and safety. It has been evident that people's and users' perspectives on technology would be drastically changed (ElArwady et al., 2024). For instance, remote monitoring tools and telehealth platforms enable continual tracking of patients' vital signs and health metrics from the comfort of their homes, empower healthcare providers to make informed decisions based on up-to-date information, and improve the quality of care delivered to patients, particularly those with chronic conditions. GPS systems can suggest the quickest routes based on real-time traffic congestion, contributing to the reduction of travel times and fuel consumption, leading to both financial savings and a smaller carbon footprint.

Considering in particular Smart Home systems, advanced sensors and automated controls, can automatically manage lighting levels and temperature according to preferences and routines for an optimal living environment (Zhou et al., 2022). Additionally, their interaction with different devices (smartwatches, mobile phones, and tablets) can leverage the user experience by providing full control and tracking of what is going on.

However, despite the benefits, IoT brings significant concerns about data privacy and cybersecurity due to the vast amounts of personal data collected and transmitted across networks. For instance, users' names, dates of birth, addresses, and credit card numbers can be typical examples of shared data among the Smart home sensors. They could be used for profiling the individuals' interactions and behavior, with a consequent privacy risk. Therefore, the use of robust security protocols for protecting against potential threats and ensuring that the adoption of IoT remains safe, secure, and effective is mandatory.

In this process, a crucial point is the level of trustworthiness guaranteed by the IoT device producers. Indeed, to reduce production costs and time, many devices are shipped without secure configurations by default and with important vulnerabilities. Moreover, given their embedded nature, these devices frequently lack regular security updates and patches after deployment. Hackers and intruders can take advantage of these vulnerabilities, potentially leading to significant financial losses that could amount to millions of dollars. Furthermore, security breaches can severely damage companies' customer relationships, ultimately eroding trust and harming brand reputation.

To mitigate these risks, this paper investigates the main cybersecurity challenges and solutions that can be considered to ensure robust security protocols and stringent compliance governance across all touchpoints associated with IoT devices (Sharma and Jindal, 2024). Specific attention will also be de-

[a] https://orcid.org/0009-0006-0489-7697
[b] https://orcid.org/0000-0003-4223-8036
[c] https://orcid.org/0000-0001-5502-303X

Waheed, T., Marchetti, E. and Calabrò, A.
Improving Cybersecurity for Smart Home Systems.
DOI: 10.5220/0013783700003985

In *Proceedings of the 21st International Conference on Web Information Systems and Technologies (WEBIST 2025)*, pages 220-227
ISBN: 978-989-758-772-6; ISSN: 2184-3252

voted to cybersecurity countermeasures by proposing a testing methodology designed for smart home device producers useful for improving their trustworthiness. By integrating perspectives from IoT specialists, testers, cybersecurity experts, and cognitive psychologists, the proposed testing platform combines technical cybersecurity evaluations, thereby promoting a comprehensive understanding of trustworthiness in smart home systems.

In its exploration, the paper overviews the following research questions (RQs):

RQ 1: Why is cybersecurity testing critical for smart home systems? We specifically investigate the consequences of insufficient testing processes for smart home systems and the potential mitigation techniques or countermeasures that can create awareness for the smart home industry to inculcate cybersecurity testing.

RQ 2: What are the current solutions for maintaining smart home cybersecurity level? In particular, we evaluate and scrutinize the current solutions and their effectiveness in maintaining cybersecurity quality and standards. It focuses on comprehending the robustness and security of the recent IoT devices and third-party software trusted by manufacturers, customers, and organizations to integrate their smart home systems.

RQ 3: What are the main research gaps? We examine existing research trends in cybersecurity for smart home systems to identify critical gaps and ensure the creation of a secure, reliable, and sustainable platform that adheres to legal, social, inclusive, and ethical benchmarks.

RQ 4: Which could be a possible solutions? We provide a robust testing methodology and framework for smart home users/industry to enhance cybersecurity quality and trustworthiness in broader perspectives.

Considering the paper structure, in Section 2, current cybersecurity challenges, testing strategies, and available solutions are presented. In Section 3, the main research gaps are discussed, and the role of cybersecurity testing is presented. The proposed testing methodology is depicted in Section 4, while in Section 5, the testing platform components are schematized. Section 6 includes the conclusion and future work.

2 RELATED WORK

To address the aforementioned research questions, we conducted a rapid review of the literature, focusing on the main databases and using the following generic query: `"(Cybersecurity AND ( Testing AND IoT AND ( Smart-home AND Systems )"`

The query was used for searching by title, abstract, and keywords on English papers from 2020 to 2025 and executed over the following electronic sources: Scopus[1], ACM Digital Library[2], IEEE eXplore[3], SpringerLink[4]. The execution provided an initial merged collection of **335** papers (excluding duplication) distributed as: ACM Digital Library - **110** papers; IEEE eXplore - **83** papers; SpringerLink - **155** papers; Scopus - **14** papers.

By reading their title, abstract, and keywords the 8 papers reported in Table 1 have been selected according to the following stringent criteria:

- Exclude papers that do not specifically concentrate on paper topics;
- Exclude papers that provide state-of-the-art reviews or surveys;
- Exclude papers that do not qualify as original or comprehensive research publications, such as forwards, editorials, monographs, books, and contributions that are not peer-reviewed or are too brief;
- Exclude short and poor-quality papers, such as those with unclear objectives or focused solutions.

Each paper provides specific considerations, such as scope, contribution, limitations, and testing strategy, as reported in the following and Table 1.

(Piasecki et al., 2021): Smart home cybersecurity standards are based on cloud-based architectures, which is a shortcoming in their longevity. Edge computing approaches like the Databox can provide advantages for security, privacy and legal compliance over cloud-based approaches. However, the current cybersecurity standards do not consider internal human threats within smart homes, such as domestic abuse and social surveillance.

(Aldahmani et al., 2023): The researchers classify the attacks into three layers (perception, network, and application) and countermeasures and security solutions have been considered for each of them. Recommended security solutions includes secure firmware updates, multi-factor authentication, and next-generation firewalls, to protect IoT devices, networks, and applications against cyber-attacks.

(Heiding et al., 2023): The researchers discovered 17 new vulnerabilities in 22 connected household devices, some of which were recognized as critical by the National Vulnerability Database (NVD).

[1]http://www.scopus.com
[2]http://dl.acm.org
[3]http://ieeexplore.ieee.org
[4]https://link.springer.com

Table 1: Rapid Review.

P.Year	Scope	Contribution	Limitation	Testing Strategy
2024	Network	Designed a network intrusion detection system (IDS).	Excessive time for training algorithm	Confusion Matrix
2023	Educational	Shaping smart-home users' attitudes toward cybersecurity awareness training.	User-centricity	Not specified
2023	Testing	Identified vulnerabilities may result in serious repercussions for residents, including the risk of an attacker obtaining physical access to the home.	Difference in expertise of student testers	Penetration Testing
2023	Security	Recommended to inculcate next generation firewalls to protect embeded IoTs in smart home systems.	Methodology Testing Platform	Not Specified
2021	Hardware	Provided technique to improve sensor identity protection for smart home systems.	Benchmark value is not determined for home settings.	Not specified
2021	Educational	Evaluating Denial of Service (DoS) and Man in the Middle (MiM) cyber-attacks for smart home systems.	Focusing on just particular IoT devices under attack.	Performance Testing
2021	Safety	Provided methodology to automatically track the location and movement of elderly people.	No sensors for monitoring oxygen level.	Machine Learning
2021	Security	Explores current smart home cybercrimes and cybersecurity standards.	Not focusing on internal human threats.	Not specified

However, the tested devices are already being sold and used worldwide, with the risk that an attacker could gain physical access to the house. Future actions to improve the security infrastructure of household IoT are necessary.

(Chen, 2021): The researchers proposed a home monitoring system that uses beacon technology to track the location and movement of elderly residents automatically and can detect potential safety issues. The system uses federated learning to enhance the object recognition capabilities of the faster R-CNN model while protecting user privacy by keeping personal data on a local server.

(Abdusalomov et al., 2024):The researchers proposed a network intrusion detection system (IDS) designed mainly for IoT-enabled smart home systems, featuring a deployment strategy that compensates for a wide range of network security challenges.

(Douha et al., 2023): The researchers investigated how cultural differences can impact smart-home users' interest in and satisfaction with non-financial rewards for cybersecurity behaviors between British and Japanese smart-home users. They claim that cybersecurity awareness training and the scope of training programs should be according to the target audience's cultural and socioeconomic backgrounds.

(Trabelsi, 2021): The researchers investigated the impact of hands-on lab exercises on vulnerability issues. They concluded that, despite positive student feedback, the students did not feel adequately prepared to assess vulnerabilities in IoT devices other than those used in the lab. Indeed, the exercises failed to cover a broader range of IoT devices and attack types, limiting the comprehensiveness of the IoT security education provided.

(Alshboul et al., 2021): The researchers proposed a 3-phase technique that significantly enhanced the protection of sensor identities in smart home area networks. The threshold value that defines the time interval for each sensor impacted the proposed technique's performance

The related work demonstrates that testing frameworks and methodologies for the cybersecurity of smart home systems are not robust and comprehensive. It is evident from Table 1 that cybersecurity for smart home systems has been improved while considering various scopes and domains. However, testing is the most under-utilized research domain, while focusing on generic penetration testing. Moreover, collaborative efforts are required to integrate testing to address modern cybersecurity challenges (Marchetti et al., 2024). The next section will explore research gaps and why we need cybersecurity testing in smart home systems.

3 RESEARCH GAPS

Diverse research gaps in smart home systems emphasize the significance of cybersecurity testing. They include:

Cyber-Attacks: It emphasizes the increasing skills of cybercriminals who exploit vulnerabilities in various interconnected devices such as smart thermostats, security cameras, and voice assistants. This situation emphasizes the need for enhanced protection and user awareness to maintain smart home systems' security.

Broader Attack Surface: It encompasses a range of devices such as smart TVs, security cameras, and smart plugs because they often operate on outdated software versions or have inadequate security proto-

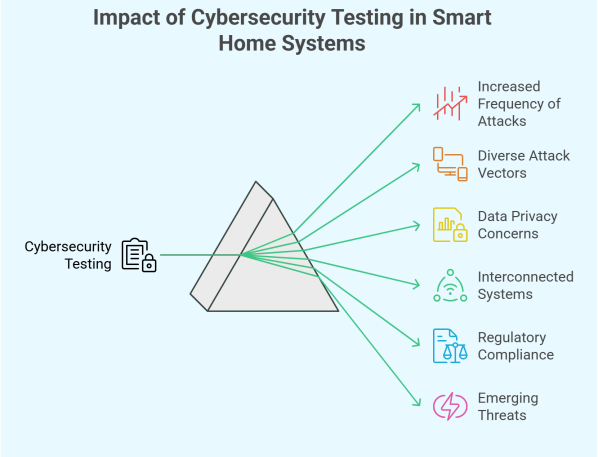

Figure 1: Impact of Cybersecurity Testing.

cols. Consequently, the risks associated with their rooted flaws increase, creating enticing possibilities for hackers to exploit.

Privacy: Management of personal data, including user needs, habits, and even sensitive information related to security and health, makes these devices vulnerable to cyber-attacks by unauthorized individuals and increases the need for robust cybersecurity measures. Common risks can be identity theft, unauthorized surveillance, and potential manipulation of smart home systems(Harkai, 2024). Prioritizing strong encryption, regular software updates, and secure password practices is essential to safeguard against these privacy challenges.

Heterogeneity: The integration of a wide range of smart devices increases the complexity and the potential points of failure within the system. Moreover, every IoT device comprises unique specifications and security protocols contributing to a heterogeneous environment (Tatipatri and Arun, 2024). However, this diversity creates significant cybersecurity vulnerabilities; for example, if one device is compromised due to invalid passwords, outdated firmware, or inherent malware, it can be a massive opportunity for cyber-attackers to compromise the entire network, gain unauthorized access to sensitive data, and control over other devices. The challenge is to ensure that all devices, regardless of manufacturer or connection type, are secured and monitored to prevent such breaches.

Regulation: government and regulatory authorities are keen to prioritize the cybersecurity of connected devices, through severe directives, standards, and regulations such as the Radio Equipment Directive (RED) for smart home systems (Mueck et al., 2025) or the EU Cyber Resilience Act (Car and De Luca, 2022). Compliance with them ensures that manufacturers implement mandatory security measures, address vulnerabilities that could compromise device functionality, protect the integrity of smart home devices, and gain prosumer trust.

Emerging Threats: Cyber threats frequently evolve with a broader range of hacking strategies and malware, raising an urgent need for cybersecurity testing to defend against these potential dangers(Bonaventura et al., 2025). Indeed, cybersecurity testing targets the discovery of weaknesses and enhances the robustness of the system against the modern attack strategies that cybercriminals might utilize. Therefore, cybersecurity testing and timely updates directly impact the safety and reliability of smart home technologies.

The importance and need for cybersecurity testing have been discussed in detail, and in the next section, we discussed limitations of current strategies and presented our testing methodology and its conceptualization.

4 TESTING METHODOLOGY

The testing methodology has been conceived while evaluating current solutions their limitations and research gaps discussed in Section 2 and Section 3. The core of our methodology comprises four attributes:

User-Centric: The focused is on prioritizing usability as a fundamental principle for fostering innovative solutions that are deeply rooted in the needs and preferences of the user (Waheed et al., 2024). By placing the end-user at the forefront of the design process, security measures can be more intuitive and seamlessly integrated into the user experience. The proposed user-centric methodology entails a thorough reevaluation of authentication methods, emphasizing ease of use. For instance, implementing biometric

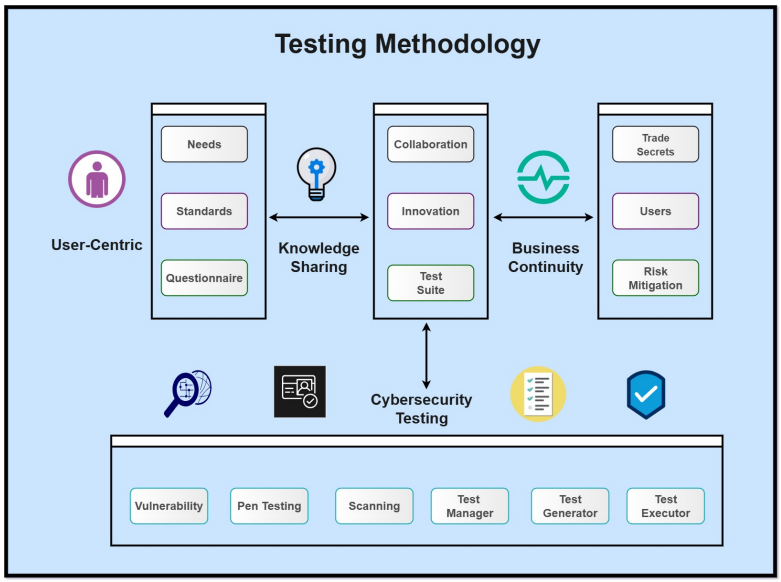

Figure 2: Testing Methodology.

authentication or multi-factor authentication options that are customizable allows users to select the security measures that best fit their individual needs. Additionally, communication regarding security notifications is designed to be clear and actionable. Users receive straightforward alerts that not only inform them of potential security issues but also guide them on how to respond effectively, thereby reducing confusion and empowering users to take control of their security settings. Overall, this approach not only enhances the security framework but also significantly improves the overall usability and satisfaction of the users interacting with the system.

Cybersecurity Testing: This process involves rigorous assessments such as penetration testing, vulnerability scanning, and threat modeling, which collectively help in revealing potential security flaws (Waheed and Marchetti, 2023). It is crucial to proactively identify and rectify these weaknesses to prevent exploitation by malicious actors, who are constantly evolving their tactics. Implementing comprehensive and proactive cybersecurity strategies is essential, and this includes conducting thorough testing throughout the entire life cycle of the system from the initial design phase to deployment and beyond. Regular and systematic evaluations not only bolster security but also enhance overall resilience against cyber threats, ensuring that protective measures remain robust against emerging risks.

Knowledge Sharing: Cultivating a robust culture of knowledge sharing and open dialogue regarding cybersecurity threats (Waheed et al., 2025) and best practices is critical for any organization. Over the years, valuable insights about potential threats and effective countermeasures have been meticulously gathered and analyzed. These findings are then shared with employees at all levels, as well as management, to significantly enhance overall productivity and efficiency through collaborative initiatives. Additionally, fostering teamwork is important for strengthening the overall security framework(Adewuyi et al., 2024). By encouraging cross-departmental cooperation and engaging with industry allies, organizations can leverage diverse perspectives and expertise, leading to innovative solutions and proactive approaches to mitigate risks.

Business Continuity: The resilience of an industry significantly enhances when organizations actively work to minimize downtime and mitigate the repercussions of critical incidents. Developing a comprehensive business continuity plan is essential; it should delineate specific protocols and strategies for responding to various cyber incidents, ranging from data breaches to ransomware attacks. Regularly updating this plan is just as important, ensuring that it reflects the latest threat landscape and incorporates lessons learned from previous incidents. A robust business continuity plan equips an organization to rebound swiftly from cyber-attacks, thereby reducing the duration of disruptions and maintaining essential operations. By implementing preventative measures, conducting regular training sessions for employees, and establishing clear communication channels, organizations can further bolster their resilience against cyber threats and ensure sustained operational integrity, even in the face of adversity.

Our holistic testing strategy strengthens defenses against cyber threats and drives continuous improvement and adaptability in IoT infastructure of smart home systems. The following section discusses the behavioral model of our testing methodology to leverage cybersecurity testing in smart home systems.

5 TESTING BEHAVIORAL MODEL

The section describes the behavioral model and workflow of our testing methodology. The testing methodology aims to facilitate the transition from conventional reactive quality control approaches to a more proactive and collaborative model. Moreover, it can assist businesses in optimizing their operations while reducing cybersecurity risks, maintaining their reputation, and enabling trust among users of industrial and commercial smart home systems. Our cybersecurity testing framework explicitly addresses the limitations of current solutions outlined in Section 4 and suggests a testing strategy and workflow for integrating advanced technologies such as all while tackling cybersecurity issues and enhancing quality for smart home users.

Our proposed SCTM (Smart Home Cybersecurity Testing Methodology) is a user-centric testing environment that promotes shared responsibility to counter modern-day cyber-attacks on smart home systems. Interestingly, Figure 3 showcases the components and the communication flow between them.

A **Test Manager (TM)** collects thorough user requirements to identify clear and specific testing objectives. It will be accomplished through questionnaires to clarify and align user expectations with their testing needs. Moreover, the component manages the testing feedback and various decisions made during the execution of testing activities for smart home systems. Furthermore, all user interactions will be performed through a dedicated User Interface (UI) (TM UI) .

The **Test Generator (TG)** aids in managing the generation and selection of test cases to the specific needs and requirements of users. Based on varying conditions, the component can suggest testing strategies and assist users in choosing the most adequate one. The test generator component will prioritize the test cases generated to identify and mitigate potential security vulnerabilities. Furthermore, executing these test cases will ensure the continuous availability, confidentiality, and overall cybersecurity of sensitive information in smart home systems.

The **Test Executor (TE)** provides testing libraries that aid in finalizing the test cases for the user smart home execution environment. Moreover, the execution environment can be supplied directly by the user, inculcating specific user requirements and preferences. Alternatively, it may be sourced from various innovative open-source proposals, ensuring a well-rounded and flexible testing strategy that accommodates user needs and scenarios.

Test Controller (TC) offers a range of testing strategies and pre-defined test cases when applicable. It assists in generating questionnaires for test managers and verifies that the test cases align with the specified requirements. Furthermore, it utilizes Generative AI to create robust test case instances and widen the scope of test suites, ensuring quality standards in light of the changing cybersecurity threats encountered by smart home systems.

It helps comprehend the effects of vulnerabilities and identify unnecessary pathways within the source code of application domains, connected IoT devices in smart home systems, and third-party libraries or APIs (Application Programming Interface). The analysis primarily utilizes path coverage testing. Furthermore, the prominent role of this component is to evaluate the test results produced by SCTM and generate reports for users through the interface of our test manager.

The **Test DB (Database) (AR)** efficiently gathers knowledge and results from testing activities. This component provides essential resources to interconnected platforms like GitHub and offers tools for creating structured questionnaires and datasets of predefined test cases. It maintains and stores test reports and user feeds; the component enhances future questionnaire design and improves the overall SCTM testing process, facilitating continuous improvement and more reliable results.

The SCTM testing platform is thoughtfully developed for smart home systems, specifically addressing the unique needs of their users. This architecture adopts a user-centered focus in cybersecurity, allowing for highly customized testing scenarios tailored to individual requirements. These scenarios effectively simulate a range of malicious behaviors and potential system vulnerabilities, creating a realistic environment. This approach encourages users to identify and understand risks and empowers them to take proactive steps to mitigate these threats, significantly enhancing their understanding of cybersecurity regulations and testing methodologies.

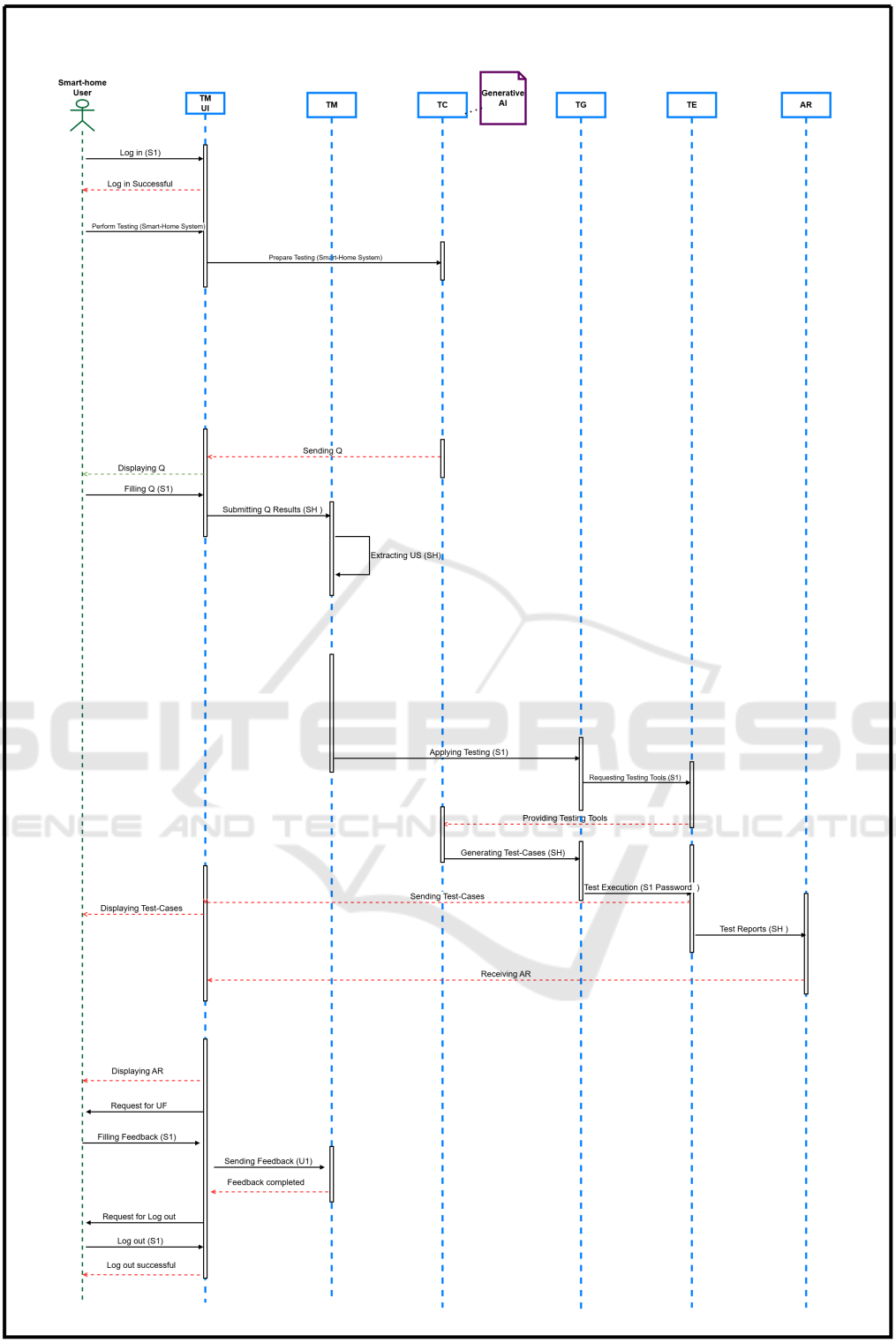

Figure 3: Behavioral Model SCTM Note: **TM**: Test Manager; **S1**: Tester-1;**Q**: Questionnaire; **UI**: User Interface; **SH**: Smart home devices; **TC**: Test Controller **TG**: Test Generator **TE**: Test Executor **AR**: Analysis and Results (Smart home device to be tested against cyber-attacks;Generating test-cases for the smart home IoT devices as per US (User Specifications).

6 CONCLUSION

As cybersecurity testing evolves through the SCTM behavioral model, it is focused on addressing the complex risks that arise from IoT devices in smart home systems. The primary objective is to encourage an environment where security is viewed as a shared responsibility among all participants, from device manufacturers to end-users.

The collaboration among stakeholders emphasizes the importance of robust testing strategies and comprehensive business continuity in case of cyber-attacks on smart home systems. By actively engaging users in the testing process, the SCTM testing model helps them gain valuable insights into their behaviors and expectations, ultimately paving the way for developing more secure and resilient smart home systems.

Future work involves testing various IoT devices and anti-theft systems as it will broaden the scope of cybersecurity testing for smart home systems through SCTM. Furthermore, the focus will be on firmware updates and innovative cyber-attacks that will make our users aware of cybersecurity challenges.

ACKNOWLEDGEMENTS

This work was partially supported by the project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NextGenerationEU.

REFERENCES

Abdusalomov, A. B., Kilichev, D., Nasimov, R., Rakhmatullayev, I., and Cho, Y. I. (2024). Optimizing smart home intrusion detection with harmony-enhanced extra trees. *IEEE Access*, 12:117761–117786.

Adewuyi, A., Oladele, A. A., Enyiorji, P. U., Ajayi, O. O., Tsambatare, T. E., Oloke, K., and Abijo, I. (2024). The convergence of cybersecurity, internet of things (iot), and data analytics: Safeguarding smart ecosystems. *World Journal of Advanced Research and Reviews*, 23(1):379–394.

Aldahmani, A., Ouni, B., Lestable, T., and Debbah, M. (2023). Cyber-security of embedded iots in smart homes: challenges, requirements, countermeasures, and trends. *IEEE Open Journal of Vehicular Technology*, 4:281–292.

Alshboul, Y., Bsoul, A. A. R., Al Zamil, M., and Samarah, S. (2021). Cybersecurity of smart home systems: Sensor identity protection. *Journal of Network and Systems Management*, 29(3):22.

Bonaventura, D., Esposito, S., and Bella, G. (2025). A case of smart devices that compromise home cybersecurity. *Computers & Security*, 151:104286.

Car, P. and De Luca, S. (2022). Eu cyber resilience act. *EPRS, European Parliament*.

Chen, M.-Y. (2021). Establishing a cybersecurity home monitoring system for the elderly. *IEEE Transactions on Industrial Informatics*, 18(7):4838–4845.

Douha, N. Y.-R., Renaud, K., Taenaka, Y., and Kadobayashi, Y. (2023). Smart home cybersecurity awareness and behavioral incentives. *Information & Computer Security*, 31(5):545–575.

ElArwady, Z., Kandil, A., Afiffy, M., and Marzouk, M. (2024). Modeling indoor thermal comfort in buildings using digital twin and machine learning. *Developments in the Built Environment*, 19:100480.

Harkai, A. (2024). Managing cyber-security risks associated with iot devices for conducting financial transactions within the smart home ecosystem. *Procedia Computer Science*, 242:200–210.

Heiding, F., Süren, E., Olegård, J., and Lagerström, R. (2023). Penetration testing of connected households. *Computers & Security*, 126:103067.

Marchetti, E., Waheed, T., and Calabrò, A. (2024). Cybersecurity testing in drones domain: A systematic literature review. *IEEE Access*, 12:171166–171184.

Mueck, M., Roberts, T., Du Boispéan, S., and Gaie, C. (2025). Introduction to the european cyber resilience act. In *European Digital Regulations*, pages 91–110. Springer.

Piasecki, S., Urquhart, L., and McAuley, D. (2021). Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards. *Computer law & Security review*, 42:105542.

Sharma, N. and Jindal, N. (2024). Emerging artificial intelligence applications: metaverse, iot, cybersecurity, healthcare-an overview. *Multimedia Tools and Applications*, 83(19):57317–57345.

Tatipatri, N. and Arun, S. (2024). A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security. *IEEE Access*, 12:18147–18167.

Trabelsi, Z. (2021). Iot based smart home security education using a hands-on approach. In *2021 IEEE Global Engineering Education Conference (EDUCON)*, pages 294–301. IEEE.

Waheed, T. and Marchetti, E. (2023). The impact of iot cybersecurity testing in the perspective of industry 5.0. In *International Conference on Web Information Systems and Technologies*.

Waheed, T., Marchetti, E., and Calabrò, A. (2024). Securer: User-centric cybersecurity testing framework for iot system. In *International Conference on Web Information Systems and Technologies*.

Waheed, T., Marchetti, E., and Calabrò, A. (2025). Vulnerability mapping and mitigation through ai code analysis and testing. *Proceedings of the 13th International Conference on Model-Based Software and Systems Engineering*.

Zhou, X., Krishnan, A., and Dincelli, E. (2022). Examining user engagement and use of fitness tracking technology through the lens of technology affordances. *Behaviour & Information Technology*, 41(9):2018–2033.